VICKIE

IST- 2001-32678

Visually Impaired Children Kit for Inclusive Education

DELIVERABLE N°: D-D.2
Secure Exchange Protocol

Report Version : 1

Report Preparation date :

Classification: Restricted

Contract Start Date: 10-01-2001, Duration:

Project Co-ordinator: Dominique ARCHAMBAULT

Partners:

CO1: UPMC (University “Pierre et Marie Curie”)

CR2: BNET (Association BrailleNet)

CR3: BRM (Regina Margherita National Library for the Blind in Monza)

CR4: CRS4 (Centro di Recerca, Sviluppo e Studi Supeiori in Sardinia)

CR6: SJS (St-Joseph’s School for the Visually Impaired)

CR7: EB (EuroBraille)

Project funded by the European Community under the « Information Society Technology » Programme

DELIVERABLES SUMMARY SHEET

Project Number:	**IST–2001-32678**
Project Acronym:	**VICKIE**
Title:	**Visually Impaired Children Kit for Inclusive Education**

Deliverable N°:	D-D.2, Secure Exchange Protocol
Due date:	
Delivery Date:	

Short Description:

This document is a first draft of the Vickie Secured Exchange Protocol (VSEP). It specifies how users can access digital documents stored in the Vickie Documents Server (VDS) from an autonomous platform or the Vickie Secured Reader. It defines the authentication procedure, an interrogation protocol to retrieve books, the cryptographic technics used to certify users and protect files efficiently. Finally, this document defines requirements to properly handle protected files and provides references to implement the VSEP on new platforms.

Partners owning:	BNET
Partners contributed:	BNET, UPMC
Made available to:	Public document

Main writers:	Benoît Guillon
Contributors:	Dominique Burger
	Dominique Archambault

Vickie Secured Exchange Protocol

Table of Contents

1. Executive summary

The VICKIE project responds to a strong demand expressed by the professionals working for visually impaired pupils or students, and these students and their families. VICKIE is a European project lead by a consortium of six partners in three European countries: France, Italy, and Ireland.

This demand appears in the context of European initiatives aiming at improving education by using information technologies, like the E-Learning Initiative which will generalize the use of computers in schools and universities over Europe.

The E-learning initiative which was adopted by the European Commission on may 24 2000 has set up quite ambitious objectives:

- to provide all schools with Internet access;
- to equip all classrooms;
- to connect all schools to research network;
- to ensure the availability of support services and educational resources on the Internet, with on-line learning platforms for teachers, pupils and parents;
- and to support the evolution of school curricula with the aim of integrating new learning methods based on information and communication technologies.

The time objective for these measures is end 2002. The objective is also to achieve a ratio of 5-15 pupils per multimedia computer by 2004.

The VICKIE project was launched to significantly contribute to realize the tremendous potential of new technologies for a greater autonomy and social integration of visually impaired students and pupils (VISP).

VICKIE aims at developing a digital information system and services that may be accessed by means of a computer equipped with the suitable inputs and outputs (Braille, speech, keyboards). Also, numerous educational existing services will be made accessible for the integration of visually impaired students.

Through international co-operation the VICKIE consortium targets additional objectives:

- services to be developed shall be in coherence with other services that are developed at an international (European) scale;
- international standards will be considered and followed;
- project will contribute to the European Design for all objectives;
- and create a sufficient market for the effective distribution of a product.

Concretely, the VICKIE project is intended to develop a technological environment that will provide three types of services for three categories of end users:

- Learning utilities for the VISPs themselves. This will include simple tools like schoolbooks and notebooks, time schedules, and mail boxes.
- Editing tools for the creation of accessible material . These tools will make it possible for sighted teachers to create documents that can be printed or read equally well, whether it on a screen, a tactile or audio device.
- Tools for improving standard electronic documents in order to make them accessible to the VISPs. These tools are intended for professionals specialized in adapting books provided by publishers for the particular needs of the VIPs.

VICKIE will develop an architecture making possible co-operative work over a network in order to strengthen the community of teachers and VISPs.

VICKIE aims at the effective distribution of a product in the context of the technologies in use in schools, taking into account the foreseeable evolution of these technologies.

The expected results for VICKIE project are a global educational environment, with a communication interface. This environment will provide:

- a range of educational services for visually impaired pupils, to access personal or global educational content ; these services are mainly based on readers, schoolbooks, time schedules and tools to organize documents, courses supports…
- A communication interface between the visually impaired pupils and their educational support: teachers, families, and sighted pupils, to exchange documents and services.

These services are provided on a local and global level:

- the local level concerns the strictly necessary tools, like reader and notebook;
- and the global level concerns general information accessible on a network, like electronic libraries and electronic schoolbooks.

A multi-modal interface implies different input and output modes: Braille, visual presentation, and voice.

2. Scope

This document describes a first draft of the Vickie Secure Exchange Protocol (VSEP).

VESP defines ways to distribute electronic documents from the Vickie Document Server (VDS) to the VISP Environment.

As this protocol to a beta test version, this document cannot be considered as a final version and will be modified if necessary. Nevertheless, it is intended to be used for technical discussions with potential partners of Vickie interested in connecting their own reading solutions on the VDS.

3. Requirements

- The VESP should modify electronic documents in order to protect intellectual property rights,
- Protected electronic documents should only be usable by the requesting user, with one of the platforms defined in the VISP Environment.
- The VESP should be available on each platform described in the VISP Environment definition. It should be based on portable and widely implemented public norms.

Protected electronic documents can be sent to:

- visually impaired pupils using secured reader software or an autonomous platform,
- teachers using secured reader software,

- transcribers using their own adaptation environment (text editor, software for Braille printing,...).

4. Documents requests and users authentication

Users allowed to access electronic documents of the VDS (pupils, teachers and transcribers) are registered in a database. Different access levels are set: pupils and teachers can access fully adapted electronic documents, whereas transcribers will download any available formats.

Authentication compares an input identity to records of the database.

4.1. From the VDS Web interface

Pupils, teachers and transcribers can access electronic documents using the Web interface of the VDS. It offers an accessible XHTML website. Books can be retrieved using different interfaces as search engines, complete catalogue or index. Results are laid out in accessible HTML tables or lists.

Each registered user receives an user name (login) and a password. To access protected electronic documents, users must enter a correct login and the corresponding password.

4.2. From an autonomous platform

An interrogation protocol is available on the VDS in order to search books using a specific user interface. Exchanges between users' platform and the VDS do not depend on a particular layout (as HTML), responses of the VDS can be parsed and displayed in a specific layout, adapted to a visual handicap.

1. The autonomous platform sends an HTTP request to a predefined URL. This request can contain following parameters:
- author: contains at least one word of the author's last name,
- title: contains at least one word of the book's title,
- isbn: contains the book's ISBN with or without hyphens,
- publisher: contains the book's publisher's full name,

2. The VDS returns an XML stream containing the list of books corresponding to the HTTP request. The XML response follows the ln-query DTD (Technical Annex 1).

3. The autonomous platform parses the XML response and displays the corresponding list of books where users can select the book and the format they wish.

4.Once a book and a format is selected, the platform sends an HTTP request to the URI included in the href attribute of the selected format element. In addition to parameters included in the URI, the HTTP request should contain following parameters:

- platformid: identifying the make and the name of the platform in use,
- serialkey: containing the unique physical serial number of the platform in use.

With an autonomous platform, users do not need to provide a login and a password. Access to electronic documents is granted if platformid and serialkey parameters match a valid account in the database.

In order to secure transmission of passwords and serial numbers, exchanges between users and the VDS may use the HTTPS transfer protocol.

5. Files protection

5.1. Users certification

A public key infrastructure has been set up to secure electronic documents delivery. The VDS acts as a certification authority and creates for each registered user:

- a 1024 bits RSA private key. This key is stored using the PEM format as shows the technical annex 2. This key identifies an user and should never transit not encrypted.
- A X509 digital certificate, signed by the VDS. This certificate contains a validity period, the RSA public key corresponding to the user's private key and information about the target user.

The private key and the digital certificate must be installed in users' platform.

5.2. Format of protected files

Files sent by the VDS follow the S/MIME (Secured / Multipurpose Internet Mail Extension) version 2 norm.

In the RFC 2311 "S/MIME Version 2 Message Specification", we read:

"S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption)."

The content-type of generated files is "application/x-pkcs-7-mime" and they are named using the "p7m" extension.

The VDS maintainers (BrailleNet and UPMC) chose tripleDES as symmetric encryption algorithm, with 128 bits session keys. It conveys a good security level to encrypted files. In case of potential security failure, another encryption algorithm will be used instead. Thus, it implies that client software decryption method should not depend on a particular symmetric algorithm.

In order to reduce size of generated files and time spent for encryption and decryption, unprotected files are archived and compressed using the zip method before encryption.

5.3. Transfer of protected electronic documents

In the RFC 2311 “S/MIME Version 2 Message Specification”, we read:

“[…] S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems.”

- Pupils and teachers using the Vickie secured reader or an autonomous platform receive protected documents via the HTTP protocol.
- Transcribers can access source files provided by publishers. Their authentication is improved by sending protected files to the e-mail address declared at inscription. Transcribers will need a compatible mailing agent (as Microsoft Outlook Express or Mozilla Mail) and their PKCS#12 digital certificate installed to decrypt files.

5.4. Protected documents handling by users' software

In both cases (autonomous platform and Vickie secured reader), users' software should:

- properly handle digital certificates and cryptographic keys,
- recognize “application/x-pkcs-7-mime” files as Vickie Secured documents,
- parse and decrypt S/MIME files (using at least tripleDES) in a buffer in volatile memory (resulting decrypted files should not be stored in temporary files of users' platform)
- unzip decrypted files in a buffer in volatile memory,
- forbid users to save files in unprotected formats.

6. Technical annex

6.1. The ln-query DTD

```
<!— ln-query represents a list of books in the VDS.  item elements
represent books, they contain bibliographical information and a list of
available formats. The href attribute of format elements is the base
URI of corresponding protected file. -->
```

```
<!ELEMENT ln-query (item)*>
<!ATTLIST ln-query
                        total   CDATA   #REQUIRED
                >
<!ELEMENT item  (title, author+, editor, formats)>
<!ATTLIST item
                        public  (1|0)   #REQUIRED
                        isbn    CDATA   #REQUIRED
                        href    CDATA   #REQUIRED
                >
<!ELEMENT title         (#PCDATA)       >
<!ELEMENT author        (#PCDATA)       >
<!ELEMENT editor        (#PCDATA)       >
<!ELEMENT formats       (format)+       >
<!ELEMENT format        (#PCDATA)       >
<!ATTLIST format
   href CDATA #REQUIRED >
```

6.2. RSA private key example

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDAFe24OSuBJHx1oVThHrKYS7gVn1oJcUaT+YG7aYjQ77OJqTtO
c23yFSCL4cQWBFoR7lwRl0R0X1mTL3S+GqptqY6OqgdhPBWLoxraWNhVaRSwdDpd
Pob6V/DPZpHDFb72267n2tNLdW14a+hY22NvifEI+CHdV8JiU699INPX/QIDAQAB
…
7RTXv7ZiVWSy5ytywEZqd9xRs5NgUC+YnuoxBGpNagWrwYVFY8oap0Ym+IKPAecX
mALDxAhcMH4G3zw9ZTuxAkBB/od+GtovRNb9cVaHkIP9yl9140naYDF/uGx8+G/3
OaQCnHb3jZGt6AXA/kvbEeFVf6UFRgFEkN0/JkpVZPcT
-----END RSA PRIVATE KEY-----

6.3. S/MIME files example

To: ...
From: ...
Subject: ...
MIME-Version: 1.0
Content-Disposition: attachment; filename="smime.p7m"
Content-Type: application/x-pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64

MIJ+0gYJKoZIhvcNAQcDoIJ+wzCCfr8CAQAxggE/MIIBOwIBADCBozCBnTELMA
kGA1UEBhMCRlIxDjAMBgNVBAgTBVBhcmlzMQ4wDAYDVQQHEwVQYXJpczE
TMBEGA1UEChMQnJhaWxsZU5ldDEaMBgGA1UECxMRTGl2cmVzIE51bWVyaXF
1ZXMxFzAVBgNVBAMTDlNl
…
+XeuACvwkyaBBxMGkLA9Cr5iBZRbxw6St+M9jjjCCI7fbXpZX//J0RZw+DVsbB8vH
mzxKDaM3VEUKPa16SXGYtMcwJkM9qyrGMzU5pDmv7TBifHbv8C2KIBcmYehvs
UFFzlhB2I9CQY6nQPQ7SWVT9zEx5Bgxg==

6.4. Links to examples of S/MIME implementations

http://www.mozilla.org/projects/security/pki/nss/smime/ (S/MIME Toolkit for Mozilla)

http://www.openssl.org (Portable open source toolkit implementing S/MIME)

http://sourceforge.net/projects/jsmime/ (an open source Java implementation of S/MIME)

http://www.isnetworks.net/smime (a commercial Java implementation)

6.5. References

http://www.w3.org/XML/ (Extensible Markup Language XML)

http://www.ietf.org/rfc/rfc2311.txt (S/MIME Version 2 Message Specification)

http://www.ietf.org/rfc/rfc2312.txt (S/MIME Version 2 Certificate Handling)

http://www.ietf.org/rfc/rfc2510.txt (Internet X.509 Public Key Infrastructure Certificate Management Protocols)

http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/ (PKCS #12 - Personal Information Exchange Syntax Standard)